

FSA Integration Partner Program
United States Department of Education
Office of Federal Student Aid



**FSA Identity and Access Management
Tools Analysis**

**Deliverable 143.1.1 Identity and Access
Management Tools – Vendor Analysis**

Version 2.0

January 30, 2004

Document Revision History

Version Number	Date	Author	Revisions Made
DRAFT Version 1.0	January 23, 2004	Anu Sharma	Initial draft
Version 2.0	January 28, 2004	Jesse Bowen	Updates to vendor analysis summaries

Table of Contents

1	EXECUTIVE SUMMARY.....	6
2	INTRODUCTION.....	9
2.1	BACKGROUND.....	9
2.2	OBJECTIVES	10
2.3	APPROACH	10
2.4	DOCUMENT OVERVIEW.....	11
3	IDENTITY AND ACCESS MANAGEMENT SOLUTION REVIEW	12
3.1	IDENTITY MANAGEMENT SYSTEMS.....	12
3.1.1	<i>Identity Management Functions and Benefits.....</i>	<i>12</i>
3.1.2	<i>Identity Management Technical Architecture.....</i>	<i>13</i>
3.1.3	<i>Identity Management Design Options</i>	<i>13</i>
3.2	WEB ACCESS CONTROL SYSTEMS.....	16
3.2.1	<i>Web Access Control Functions and Benefits</i>	<i>16</i>
3.2.2	<i>Web Access Control Technical Architecture</i>	<i>16</i>
3.2.3	<i>Web Access Control Design Options.....</i>	<i>17</i>
4	IDENTITY MANAGEMENT.....	20
4.1	INTRODUCTION TO IDENTITY MANAGEMENT PRODUCTS	20
4.1.1	<i>Control/SA - BMC</i>	<i>21</i>
4.1.2	<i>IdentityMinder – Netegrity</i>	<i>22</i>
4.1.3	<i>Xellerate – Thor.....</i>	<i>23</i>
4.1.4	<i>Identity Manager – Tivoli/IBM.....</i>	<i>24</i>
4.1.5	<i>Lighthouse – Waveset.....</i>	<i>25</i>
4.2	IDENTITY MANAGEMENT PRODUCT SELECTION CRITERIA.....	26
4.3	SUMMARY EVALUATION MATRIX – IDENTITY MANAGEMENT	28
4.4	IDENTITY MANAGEMENT PRODUCT ANALYSIS	30
4.4.1	<i>Product Functionality.....</i>	<i>30</i>
4.4.2	<i>Product Flexibility.....</i>	<i>30</i>
4.4.3	<i>Deployment Effort.....</i>	<i>30</i>
4.4.4	<i>Operational Effort</i>	<i>31</i>
4.4.5	<i>Vendor Stability.....</i>	<i>31</i>
4.4.6	<i>Identity Management Vendor Recommendations</i>	<i>31</i>
5	WEB ACCESS CONTROL	33
5.1	INTRODUCTION TO WEB ACCESS CONTROL PRODUCTS	33
5.1.1	<i>SiteMinder – Netegrity.....</i>	<i>34</i>
5.1.2	<i>NetPoint – Oblix</i>	<i>35</i>
5.1.3	<i>ClearTrust – RSA.....</i>	<i>36</i>
5.1.4	<i>Access Manager – Tivoli/IBM</i>	<i>37</i>
5.2	WEB ACCESS CONTROL PRODUCT SELECTION CRITERIA.....	38
5.3	SUMMARY EVALUATION MATRIX – WEB ACCESS CONTROL.....	40
5.4	WEB ACCESS CONTROL PRODUCT ANALYSIS	42
5.4.1	<i>Product Functionality.....</i>	<i>42</i>
5.4.2	<i>Product Flexibility.....</i>	<i>42</i>
5.4.3	<i>Deployment Effort.....</i>	<i>42</i>
5.4.4	<i>Operational Effort</i>	<i>42</i>
5.4.5	<i>Vendor Stability.....</i>	<i>42</i>
5.4.6	<i>Web Access Control Vendor Recommendations</i>	<i>43</i>
6	CONCLUSION AND NEXT STEPS.....	44

APPENDIX A: ENROLLMENT AND ACCESS MANAGEMENT SOLUTION VISION	46
APPENDIX B: FSA SECURITY AND PRIVACY ARCHITECTURE FRAMEWORK.....	47
APPENDIX C: SECURITY WORKING GROUP ROSTER	48
APPENDIX D: SECURITY WORKING GROUP PRESENTATION	49
APPENDIX E: VENDOR EVALUATION CRITERIA MATRIX	50

Figures

Figure 1 – Vendor Presentation Schedule	11
Figure 2 – Generic Architecture of Identity Management Systems.....	13
Figure 3 – “Agent-based” Identity Management Architecture	14
Figure 4 – “Agentless” Identity Management Architecture	15
Figure 5 – Comparison of agent-based and agentless approaches to identity management system architecture	15
Figure 6 – Generic Architecture of Web Access Control Systems	17
Figure 7 – “Web agent” Based Access Control	18
Figure 8 – “Reverse Proxy” Based Access Control.....	18
Figure 9 – Comparison of web agent and reverse proxy approaches to web access control system architecture.....	19
Figure 10 – Identity Management Product Selection Criteria	27
Figure 11 – Summary Evaluation Matrix Key: Identity Management	28
Figure 12 – Summary Evaluation Matrix: Identity Management	29
Figure 13 – Web Access Control Product Selection Criteria.....	39
Figure 14 – Summary Evaluation Matrix Key: Web Access Control.....	40
Figure 15 – Summary Evaluation Matrix: Web Access Control.....	41
Figure 16 – FSA Identity and Access Management Solution Vision	46
Figure 17 – FSA Security and Privacy Technical Architecture.....	47
Figure 18 – Security Architecture Workgroup Roster	48

1 Executive Summary

The Identity & Access Management Tools Analysis is designed to support FSA in the selection and testing of Identity Management and Web Access Control technologies. The goal of this effort is to analyze the capabilities of existing commercial security technologies for satisfying previously defined FSA business objectives. This effort resulted from the preliminary activities of the Data Strategy Enrollment and Access Management and the Security and Privacy Architecture Framework tasks. The major business objectives addressed in this evaluation are intended to satisfy FSA desires to:

- Manage security functions across environments and platforms.
- Reduce the number of trading partner passwords (provide single sign-on).
- Provide self-service functions (password reset, user information updates, etc.).
- Allow delegated security administration of selected tasks.
- Synchronize passwords across multiple systems and platforms.
- Provide tools to implement Web Services Security standards.
- Provide flexible authentication methods for web applications.

The first phase of the Identity & Access Management Tools Analysis, documented in this deliverable, is the Vendor Analysis. This effort completes several major tasks, including:

- Documenting a comprehensive list of relevant Identity Management and Web Access Control Solutions.
- Identifying five Identity Management and four Web Access Control products that represent market-leading solutions.
- Arranging on-site presentations to FSA by the selected vendors.
- Establishing criteria for evaluation of products and vendors.
- Documenting major advantages and disadvantages of each product.
- Recommending solutions for more extensive demonstrations and further analysis.

After documenting the set of relevant Identity Management and Web Access Control Solutions, the team narrowed down the list based on a subset of the criteria such as vendor and product stability, market share, and functionality. The following five Identity Management products were investigated further:

- Control-SA (BMC)
- IdentityMinder (Netegrity)
- Lighthouse (Waveset)
- Tivoli Identity Manager (IBM)
- Xellerate (Thor)

The four Web Access Control solutions reviewed by the team are:

- ClearTrust (RSA)
- NetPoint (Obliv)
- SiteMinder (Netegrity)
- Access Manager (Tivoli/IBM)

The team judged the products in several categories based on established evaluation criteria areas such as:

- Vendor Background: vendor profile, market position
- Identity Management Functional Requirements – provisioning, delegated administration, security policy, and self-service functions, auditing and reporting.
- Web Access Control Functional Requirements – user authentication, single sign-on, user access control, user auditing
- Identity Management and Web Access Control Technical Requirements – platform, integration, standards support.

The major advantages and disadvantages of each product were documented and evaluated. Several solutions in each category are recommended for further product demonstrations and analysis:

Identity Management:

1. *Waveset Lighthouse* offers a good compromise between features, deployment flexibility, and vendor stability.
2. *IBM's Tivoli Identity Manager* is a more complex product to deploy and maintain, but has the advantage of a very stable support structure.
3. *BMC's Control-SA* did not rank as high as the previous two products because of its more complex deployment and maintenance requirements.

The original Task Order for this project recommended selecting two Identity Management products to invite for more extensive demonstrations. However, because Control-SA was licensed in the past by FSA, it was added to the list of vendors to invite for on-site demonstrations.

Web Access Control:

1. *Netegrity SiteMinder* offers a stable product with a comprehensive set of authentication, authorization, and single sign-on features.
2. *IBM Tivoli Access Manager* is based on a reverse-proxy architecture and has a comprehensive feature set, although its complexity has led to complicated deployment efforts for some customers.
3. *RSA ClearTrust* has a smaller installed base than either of the two previous products, but is stable and supported by a vendor with a very strong presence in the security product market.

The RSA product was added to this list to provide an alternative to the SiteMinder product in the event that the reverse-proxy architecture is found unsuitable for the FSA environment.

Industry analyst research supports the recommendation of these Identity Management and Web Access Control tools for further evaluation. Each of the tools is rated among the top of their peer group and possesses the functionality necessary to meet or exceed FSA Business Objectives.

2 Introduction

2.1 Background

The Task Order Identity & Access Management Tools Analysis (TO143) builds on the preliminary activities of the Data Strategy Enrollment and Access Management (TO123)¹ and Security and Privacy Architecture Framework (TO124)² tasks.

As a part of Data Strategy Enrollment and Access Management initiative, representatives from various systems gathered, analyzed, and refined business objectives and high-level requirements and formulated possible solution options as a high-level design. The Enrollment and Access Management Solution Vision is shown in Appendix A. Some of the requirements that relate to identity management solutions include:

- Manage security functions across environments and platforms
- Reduce the number of passwords (simplified sign-on)
- Provide self-service functions (registration, password reset, etc.)
- Allow delegated security administration of selected tasks
- Synchronize passwords across multiple systems and platforms

Some of the requirements for that relate to Access Control tools include:

- Reduce number of User IDs and passwords for web based applications (Single Sign-On).
- Provide tools to implement Web Services Security standards.
- Provide flexible authentication methods for web applications.

Due to the maturity of current Identity Management and Web Access Control tools, the Data Strategy Enrollment and Access Management project recommended the evaluation of Commercial Off-The-Shelf (COTS) solutions rather than custom development.

Security and privacy architecture objectives were identified through workshops and integration meetings with FSA business and technical leaders. Security objectives surrounded managing, administering, and auditing access, establishing methods to protect data and infrastructure, and signing transactions. The result of the task order was the FSA Security and Privacy Architecture Framework as shown in Appendix B. A primary outcome from that effort was the recommendation that FSA deploy security infrastructure

¹ TO123 Data Strategy Enrollment and Access Management deliverables included:
123.1.27 Access Management Business Objectives (submitted on 6/30/03), and
123.1.29 Access Management High-Level Design (11/30/03).

² TO124 Security & Privacy Architecture Framework included:
124.1.1 Interim Security and Privacy Architecture Report (submitted on 4/04/03),
124.1.2 Final Security and Privacy Architecture Report (5/30/03), and
124.1.3 Security and Privacy Architecture Framework Specification (5/30/03).

services to provide Web Access Control and Identity Management functions across FSA systems.

2.2 Objectives

The Tools Analysis task order was created to support FSA selection and testing of Identity and Access Control technologies to satisfy FSA Business Objectives. By assisting FSA in identifying the relevant advantages and disadvantages of COTS solutions, FSA will be in a better position to make informed decisions about how to best adapt FSA enterprise security processes and architecture to meet the defined requirements. The Tools Analysis Team will help FSA:

- Evaluate leading vendor offerings in the Web Access Control and Identity Management technology categories.
- Select products in each category for an on-site prototype integration with a sample FSA system (ezAudit).
- Identify considerations and impacts for future FSA deployment.

This Vendor Analysis document is the result of extensive review of Identity Management and Access Control tools by an FSA team comprised of CIO and Business Unit Organization leaders. Accenture contractors assisted this effort with information gathering and management of the technology analysis. Note, however, that product selection decisions are the sole responsibility of FSA.

2.3 Approach

The Tools Analysis is divided into three major phases:

- Vendor Analysis Phase – This phase will establish criteria for a vendor evaluation, identify market leading solutions, and select products for on-site evaluation.
- Product Options Phase – An on-site vendor evaluation and testing will be conducted, vendor solutions will be analyzed, and products will be selected for a prototype.
- Prototype Phase – In this phase, the team will prototype and test the Identity Management and Web Access Control components in the FSA development environment against FSA business objectives.

An initial project meeting was held on December 9, 2003 with the Security Working Group. The Security Working Group was formed to review the vendor analysis, review team progress, and provide input to ensure the Identity Management and Web Access Control solutions meet business needs. The group is composed of participants from various CIO, application, and business teams. The Security Working Group roster is included in appendix C.

During the Tools Analysis phase, the team documented a preliminary list of Identity Management and Web Access Solutions of 10-12 systems per product type. Each

offering was thoroughly reviewed and screened on a subset of criteria. Only the financially strongest companies with the most robust product offerings were invited for an on-site presentation on their product. Through this process, seven different vendors were selected to present five Identity Management and four Web Access Control solutions to the FSA team. These vendors and products are shown in Figure 1.

Date	Product	Date
Waveset	Lighthouse	12/15/03
Tivoli/IBM	Access Manager Identity Manager	12/17/03
Netegrity	IdentityMinder SiteMinder	12/18/03
RSA	ClearTrust	12/18/03
Thor	Xellerate	12/18/03
Oblix	NetPoint	1/9/04
BMC	Control-SA	1/13/04

Figure 1 – Vendor Presentation Schedule

The team evaluated the products in several categories based on established criteria and recommended a subset of products in each category for on-site demonstrations.

A project briefing was held with the Business Integration Group on January 6, 2004. A project update was given to the Security Working Group on January 14, 2004 and with the CIO organization on January 15, 2004. A copy of the January 14, 2004 Security Working Group presentation is available in Appendix D.

2.4 Document Overview

This deliverable summarizes the results of the Vendor Analysis phase of this project. Subsequent sections contain the following content:

Section 3 – Overview of technologies available for identity and access management, and the major architecture approaches employed by commercial vendors.

Section 4 – Identity Management product summaries and recommendations

Section 5 – Web Access Control product summaries and recommendations

Section 6 – Conclusion and Next Steps

Appendix – Detailed product analysis information and background materials.

3 Identity and Access Management Solution Review

The Access Management capability of the overall FSA Enrollment and Access Management Solution Vision developed in TO 123³ is composed of two major components: Identity Management and Web Access Control. This section provides an overview of the technical architectures of COTS software packages for these two different but related functions. The discussion below also defines the major design approaches for each capability as an aid to understanding the analysis of differences in the development, deployment, and operation of these security tools.

3.1 Identity Management Systems

3.1.1 Identity Management Functions and Benefits

Identity Management solutions provide several critical enterprise functions for user administration and management across multiple systems. These functions automate the process of creating and maintaining identity information, but do not affect existing runtime security operation of the system, such as authentication and authorization. Identity Management solutions provide several types of functionality:

- **User Administration** – User Administration manages the provisioning, maintenance, and deletion of a user’s identity information through a central repository. Either rules, based on business processes and requirements, or Roles Based Access Control (RBAC) methods, based on sets of access privileges assigned by job functions, can be used to govern user access rights.
- **Delegated Administration** – Delegating administration functions allows administrative tasks (such as adding a new user or changing access) to be performed by approved external administrators.
- **Audit** – An Identity Management System communicates with the security functions of each information system and provides centralized security auditing and reporting capabilities.
- **Integrated Security Workflow Capabilities** – Identity Management solutions offer pre-configured workflows for key security tasks such as approving new users.
- **Password Management** – Identity Management systems can enforce security policies (such as password policies), automate password resets, and synchronize passwords.

Identity Management primarily benefit system administrators in the form of cost savings for operations such as password resets and improved audit capabilities. Some of the major benefits include the ability to:

- **Integrate with and manage security functions across environments and platforms** to enable development of enterprise user access roles.
- **Improve the accuracy of assigning and monitoring access privileges across multiple systems.**

³ Documented in deliverable 123.1.29 – Access Management High Level Design (11/30/03)

- Reduce the number of user passwords (simplified sign-on) through automating synchronization of passwords across multiple systems.
- Deploy self-service functions such as automated password reset and user updates of demographic information.
- Allow delegation selected security administration tasks to authorized remote administrators.
- Enhance enterprise auditing and reporting capabilities through creation of cross-system access reporting.

3.1.2 Identity Management Technical Architecture

Figure 2 shows typical elements of a generic Identity Management system. Major components include the primary Identity Management server, a user account database, and mechanisms to mediate communications with the security databases or security functions of the systems being managed. The Identity Management server contains the logic to provide a centralized administration interface, and performs the user account provisioning function. Additional program modules may optionally provide password management and security approval workflow functions. The User Account Database stores and manages information that links individual users to their accounts on multiple systems across the enterprise. A communications subsystem manages the exchange of account and system information between the Identity Management server and each target system.

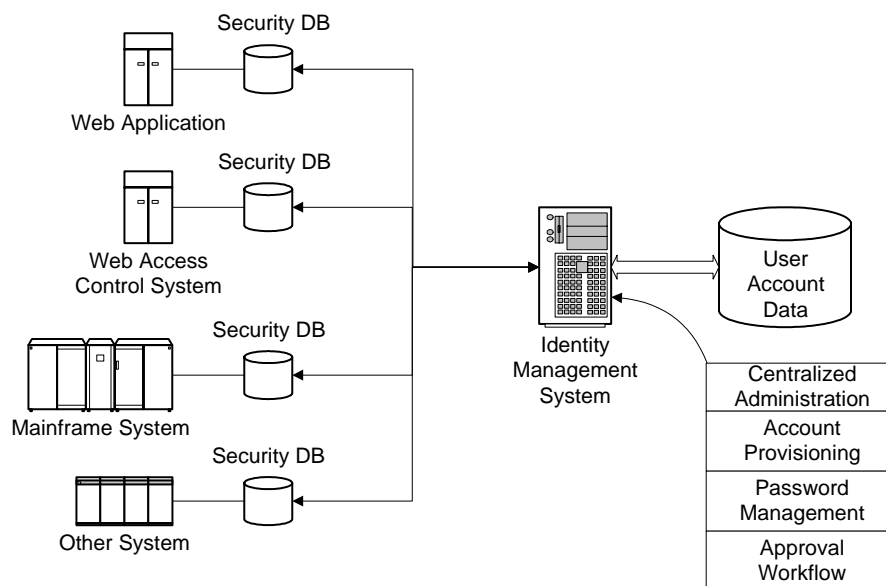


Figure 2 – Generic Architecture of Identity Management Systems

3.1.3 Identity Management Design Options

The major design approaches for identity management systems are shown in Figures 3 and 4. The original architecture for provisioning user accounts is shown in Figure 3. This design centralizes user administration relied on deployment of software “agents” on each platform or system to be managed. The agent provides access to system or

application functions needed to configure user accounts or extract user security data from the target system. It also manages the communication link to the central identity management server. While providing a rich set of functionality through its close integration with the underlying target system or application, agents must be installed, tested for interactions, and monitored. This effort represents ongoing maintenance overhead whenever the target system, the adapter, or the identity management system is upgraded. In addition, new agents must also be coded and tested for custom systems that cannot use agents developed for standard commercial systems. These factors have resulted in a history of long deployment cycles and complex efforts for large implementations of commercial products using this design approach.

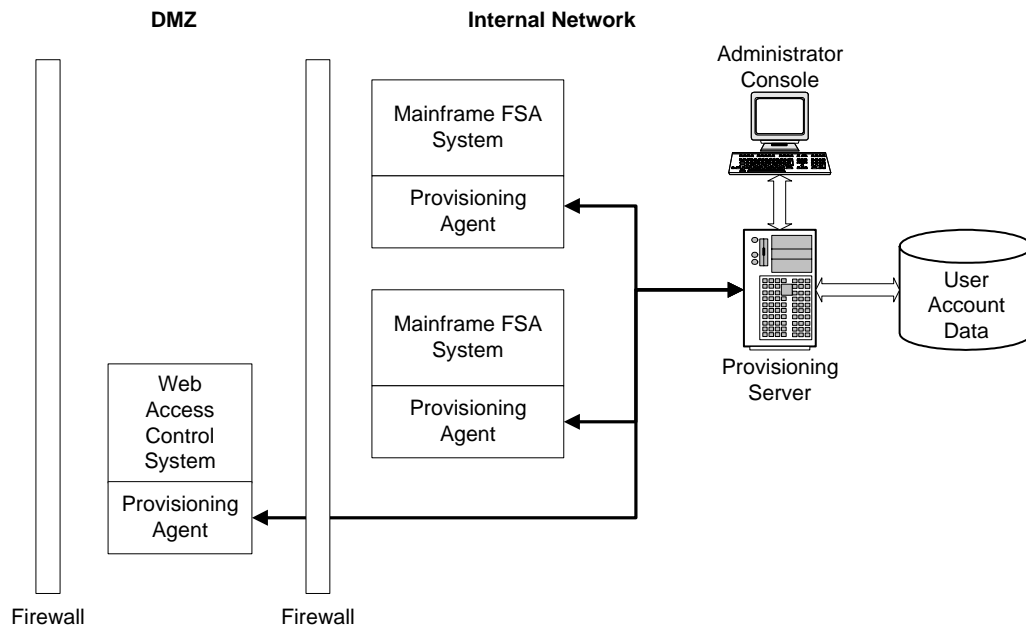


Figure 3 - "Agent-based" Identity Management Architecture

As an alternative to agents, a more recent approach has been developed that provides communications to target systems through adapters integrated into the identity management server itself (Figure 4). This approach relies on native interfaces, when available, that are provided by the target system (e.g., command line interfaces, APIs, terminal sessions). The advantage of this approach is that it greatly decreases development time and avoids the need to deploy new and potentially disruptive code on the systems being managed. The interface adapters are also typically easier to develop for systems not already supported.

The trade-off for the agentless approach is some decrease in the level of integration with the target system, and a consequent decrease in access to more complex security functions. In response to the advantages of the agentless approach, commercial vendors who originally offered agent-based products have started to embrace the lower impact approach of the newer architectures. However, most of the original products in this space still rely heavily on agents to achieve advertised functionality.

These architectural differences should be given prominent consideration during product selection but do not solely justify one product over another. The table in Figure 5 summarizes the advantages and disadvantages of these two architectural approaches.

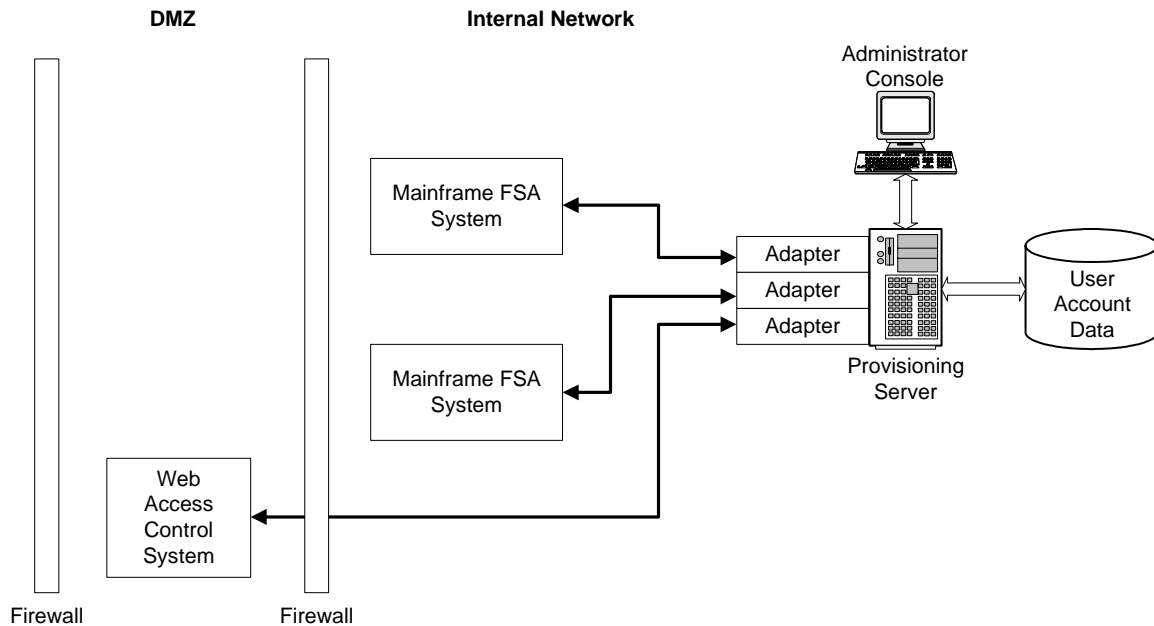


Figure 4 – “Agentless” Identity Management Architecture

	Agent-based	Agentless
Advantages	<ul style="list-style-type: none"> • Tighter integration with managed system – more complete access to internal functions 	<ul style="list-style-type: none"> • Faster, easier implementation • Usually stores less user information in central user database • Development of system adapters more rapid and easier
Disadvantages	<ul style="list-style-type: none"> • More complex implementation and maintenance (code must be deployed, tested, and monitored on each managed system) • Usually stores large amount of user data in central user database • Development of agents for new or custom systems requires significant development effort 	<ul style="list-style-type: none"> • Limits on internal functions available from managed systems

Figure 5 – Comparison of agent-based and agentless approaches to identity management system architecture

3.2 Web Access Control Systems

3.2.1 Web Access Control Functions and Benefits

Web Access Control systems provide flexible runtime authentication services and access control for Web Applications. These functions provide Single Sign-On and other functions which improve the experience of external users. Web Access Control solutions provide several types of functionality:

- **Web Authentication** – Web Authentication validates the identity of the user, such as with a UserID and password. Web Authentication can also provide Web Single Sign-On which eliminates the need for a user to reenter authentication information when switching from one web application to another.
- **Authorization** – Authorization components validate that a user has approved privileges to access specific protected resources. Often, authorization functions are split between WAC systems and target applications to allow for quicker implementation or more fine grained authorization functions.
- **Repository Components** – Repository components store authentication and authorization information and can be used to exchange information with Identity Management systems or other data stores (such as LDAP directories).

Web access control systems provide multiple benefits for both the user and FSA. This technology can:

- Reduce the number of User IDs and passwords and enable Single Sign-On functions for web-based applications.
- Provide tools to implement Web Services Security standards.
- Provide flexible authentication methods for web applications.
- Allow security functions (e.g., authentication, authorization, auditing) to be implemented as consolidated infrastructure services instead of duplicated functions within each web application.
- Decrease the time required for design and implementation of new web applications by greatly reducing development time associated with security functions.
- Provide a single database for storing security data (user information, authentication information, access rules, etc.) to simplify security administration and maintenance for web applications.
- Increase system flexibility by providing access to complex security functions when needed without requiring custom development (e.g., strong authentication, digital certificate functions, e-Authentication compatibility)

3.2.2 Web Access Control Technical Architecture

Figure 6 depicts the major components of a typical web access control architecture. The major features include 1) the web access control policy server, and 2) a database for storing user information, user credentials, and information about authorization rules and

policies. The web access control server provides a central point of control for the user login process and mediates user authentication functions for web applications controlled by the system. As a result, user credentials can be created and communicated to implement single sign-on functions and avoid the need for users to authenticate to each web system. The User and Policy database is often implemented as an LDAP directory server, although in most cases a standard commercial relational databases can also be used. This database stores user account information and the data needed to validate user authentication credentials. It also manages user access authorization information, including role-based access control attributes and rules that implement dynamic rules for making access decisions.

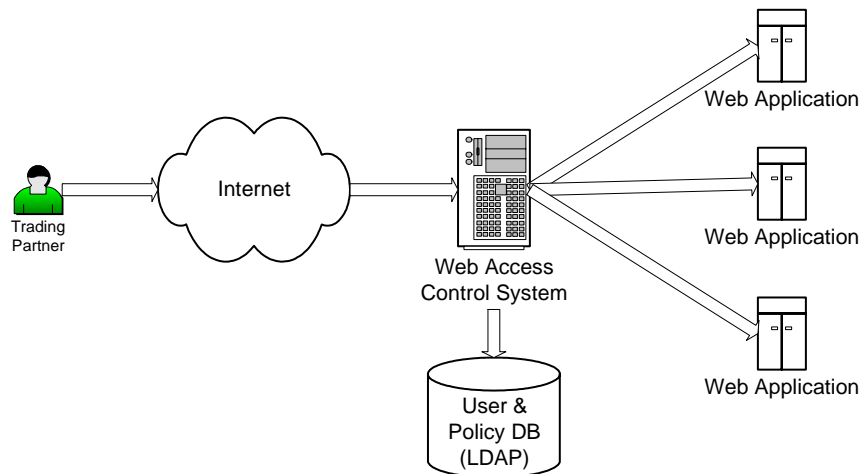


Figure 6 – Generic Architecture of Web Access Control Systems

3.2.3 Web Access Control Design Options

There are two major architectures in common use for web access control systems, as shown in Figures 7 and 8. The “web agent” approach shown in Figure 7 employs an http filter on the web server being protected. The filter intercepts requests for web pages or resources, and checks whether they have been designated as protected. If so, the filter initiates a user login step, communicates with the policy server to check the user credentials, and sends an authorization session token to the user’s web browser upon successful login. This token is inspected during subsequent requests for specific web resources for any of the protected web applications. The token is used to check authorization rules in the policy database to determine if access for the requested resource is allowed.

An alternate approach to protect web applications is shown in Figure 8. This design requires installation of a reverse proxy server, typically in an additional DMZ network layer protected by firewalls. The reverse proxy server intercepts all requests for protected resources, mediates login steps, and communicates with the policy server to make authorization decisions. A session token is also sent to the user’s browser to help maintain session state.

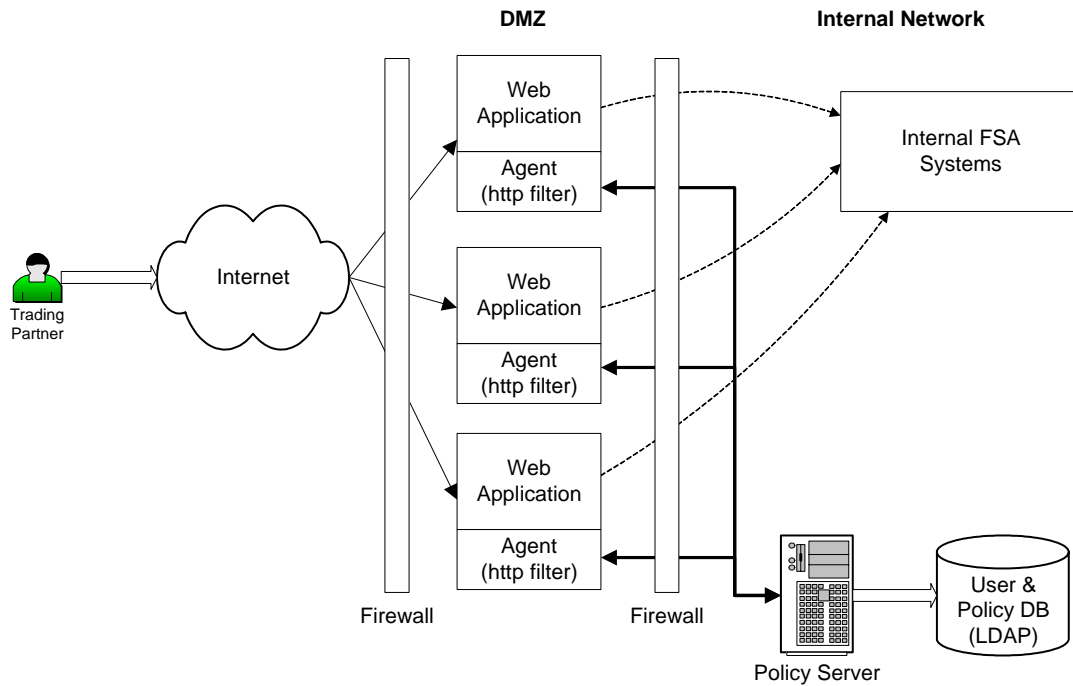


Figure 7 – “Web agent” Based Access Control

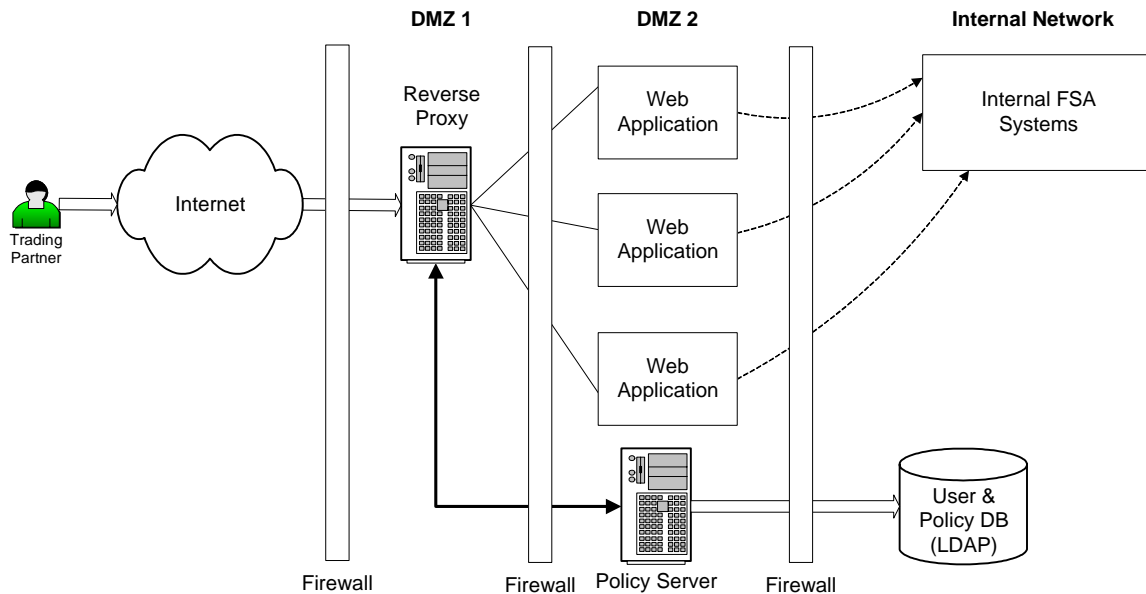


Figure 8 – “Reverse Proxy” Based Access Control

The web agent/http filter approach is typically quicker and easier to implement than the reverse proxy architecture. It requires fewer changes to the network infrastructure, and is generally easier to maintain. This design approach also has some advantages in terms of

scaling, since only the policy server need be replicated as traffic demands increase; the http filters will scale automatically as the number of web servers increases to adjust to traffic demand.

The reverse proxy architecture provides some increment in resistance to network attack since it deploys an additional network layer. However, the added network segment will require new server and network hardware, and increases the complexity of deployment and maintenance. The reverse proxy also represents additional hardware and software that will need to be added to scale for supporting higher traffic demands.

The differences between the web agent and reverse proxy approaches, while important, are not by themselves sufficient to make the selection of products. The differences, however, should be given prominent consideration. The table below summarizes the advantages and disadvantages of each of these approaches.

	Web Agent	Reverse Proxy
Advantages	<ul style="list-style-type: none"> • Easier, faster implementation • Simpler maintenance • Maintains current network architecture • Scales with web server capacity and by adding additional policy servers 	<ul style="list-style-type: none"> • Increased resistance to network attack
Disadvantages	<ul style="list-style-type: none"> • Requires installation of web server filter on web servers and/or application servers being protected 	<ul style="list-style-type: none"> • Greater complexity - requires additional network/firewall layer • More expensive to deploy and maintain • Scales by adding additional proxy servers and policy servers

Figure 9 – Comparison of web agent and reverse proxy approaches to web access control system architecture

4 Identity Management

4.1 Introduction to Identity Management Products

During the Tools Analysis phase, the team documented a preliminary list of Identity Management and Web Access Solutions of 10-12 vendors per product type. Initial Identity Management solutions are:

- Control-SA (BMC)
- eProvisioning (Business Layers – now purchased by Netegrity)
- eTrust Identity Management (Computer Associates)
- IdentityMinder (Netegrity)
- Lighthouse (Waveset)
- .NET Passport (Microsoft)
- NetPoint Identity Manager (Obliv)
- SunONE Identity Server (Sun)
- Tivoli Identity Manager (IBM)
- Xellerate (Thor)

Each offering was initially reviewed and screened on a subset of criteria. Several products were eliminated from initial consideration because of market position or technology orientation. Business Layers, which markets the eProvisioning product, was recently purchased by Netegrity, and is marketed by them as part of the IdentityMinder product line, so it is considered under that banner. The eTrust Identity Management product has relatively few implementations outside of organizations that make use of Computer Associates systems management software. Microsoft's .NET Passport and related identity management software is oriented toward Microsoft development and server platforms. The Obliv NetPoint product provides identity management functions, but only for web applications, so it was not considered as an enterprise identity management solution (it was considered in the Web Access Control category, however.) The SunONE Identity Server product is very new to the marketplace and has a small installed base.

Given the above considerations, the five vendors with the strongest products and market presence were selected for further consideration:

- Control-SA (BMC)
- IdentityMinder (Netegrity)
- Lighthouse (Waveset)
- Tivoli Identity Manager (IBM)
- Xellerate (Thor)

4.1.1 Control/SA - BMC

Company Overview

Texas based BMC Software, Inc. is a systems software vendor that delivers comprehensive enterprise management solutions. The company focuses on providing software solutions that enhance the availability, performance and recoverability of its customers' business-critical applications to help them better manage their businesses. BMC has been in the software industry for 19 years, is one of the world's largest independent software companies, and is a fortune 500 company. BMC acquired the Control-SA product from New Dimension Software in 2000.

Product Description

BMC's CONTROL-SA product is an identity management and provisioning solution that consists of the following components.

- Enterprise Security Station (ESS): This is the central administration database that holds a list of all employees (known as Enterprise Users). Each employee in the company has an EU account. This central account is linked to every other account that the user has on various systems around the company (i.e. Windows domain account, Unix account, etc.) through the use of SA Agents.
- SA Agents: Software installed on target systems that communicates with various platforms and manage that system (add or delete accounts, update password, etc).
- Control/SA Passport: Passport is part of the Control/SA product suite that provides a web based interface for users, from which they can change or synchronize their password throughout all systems.

Pros

- BMC is a well established software provider
- Control-SA was one of the first Identity Management products, initially brought to market over seven years ago.
- Control-SA agents provide immediate updates of changes in target systems.
- Control-SA has several Government and Financial Services clients

Cons

- Control-SA's market share has been steadily declining in recent years
- Control-SA prefers agents on managed systems which can lead to greater complexity and, therefore, additional deployment and operational effort.
- Agents require greater skill and effort to develop and maintain compared to agentless products.
- Control-SA can be difficult to customize, and has a history of difficult implementations at some existing clients
- Although there is a Control-SA workflow module, it lacks flexibility and functionality so BMC has partnered with a third-party vendor to provide workflow functions (Business Layers, recently acquired by Netegrity)

4.1.2 IdentityMinder – Netegrity

Company Overview

Netegrity, Inc., founded in 1986, is a publicly held company headquartered in Waltham, Mass. Netegrity solutions are licensed to more than 250 million users at nearly 700 organizations worldwide, including more than half of the Fortune 100. Netegrity is a mature company in the security tools market space, with a large corporate and government customer base. Netegrity customers for its other security products include Aetna, American Express, Bank One, E*TRADE, General Electric, the Internal Revenue Service, and Wells Fargo. The IdentityMinder provisioning engine consists of an OEM version of the Business Layers provisioning solution, for which there are no existing customers with production implementations. Netegrity recently acquired Business Layers.

Product Description

The IdentityMinder product consists of two major editions as described here:

- IdentityMinder Web Edition provides role-based access control, delegated administration, self-service of user profiles and passwords, integrated workflow, and a structured environment for administration and user management in the Web environment. IdentityMinder and SiteMinder tie the key components together to produce a centralized identity and Web access management system.
- IdentityMinder (Provisioning Edition) manages account creation to legacy and backend systems. The system provides delegated administration; rules based access, password synchronization and auditing/reporting capabilities for legacy, mainframe, and other “non-Web” systems. Netegrity’s provisioning engine is based on the Business Layers solution, a company that Netegrity recently acquired.

Pros

- The web functions of the IdentityMinder version of the software is tightly integrated with Netegrity SiteMinder Web Access Control product – uses same policy engine and directory information
- Integrated workflow engine automates security approval

Cons

- IdentityMinder by itself does not provide general purpose provisioning functions, which requires the IdentityMinder (Provisioning Edition) product.
- The IdentityMinder (Provisioning Edition) product was recently acquired through purchase of Business Layers. There is currently insufficient information available on the new product to analyze it completely.
- Small installed base and little history of support for the product by Netegrity.
- Architecture is not as robust as some other products.

4.1.3 Xellerate – Thor

Company Overview

Based in New York City, Thor Technologies, Inc. is a leading provider of access rights management and provisioning solutions for enterprises. Thor's first 10 years as a company were focused on providing provisioning solutions within the telecommunications industry. Thor is now offering their solution to a broad range of enterprises, and including large customers such as Nextel and Lehman Brothers. The Thor product was recently selected to provide identity management services for the U.K. National Health Service.

Product Description

Thor's flagship product, Xellerate, is an automated platform that centrally manages access rights and provisioning in the enterprise by helping to:

- Define and streamline multiple and complex approval processes into a unified process
- Automatically execute the entire process from end to end according to business rules that reflect corporate policies, or set Xellerate to interact with a hierarchy of authorizing approvers
- Integrate new applications for delivery and link all resources into a centrally managed portfolio
- Monitor individual service requests, meter resource usage, and generate historical reports
- Enable instant access termination, strengthening security by protecting against unauthorized access to corporate information assets.

Pros

- Has a unique GUI-driven Adapter Factory to auto-generate adapter code and reduce manual programming to build or maintain adapters for target systems.
- Offers flexible interface customization and easy integration.
- Provides “reverse provisioning” roll-back capabilities to provide robust transactional integrity for workflow or coding errors.
- Flexible interface customization.
- Delegated Administration is independent of the Enterprise directory tree.
- Workflow definitions can be imported from Visio and other file formats

Con

- Small but growing installed base.
- Small, privately-funded company, raising concerns about capacity to scale and long-term viability.
- Does not run on the HP-UX platform.

4.1.4 Identity Manager – Tivoli/IBM

Company Overview

IBM's security software offerings, marketed by its Tivoli division, provide an end to end package of tools for integrating, managing, and securing an enterprise's electronic infrastructures and processes. In September of 2002 IBM acquired Access360, a private maker of provisioning software, in a move to expand upon and strengthen IBM's identity management offerings. Both the Access Manager and Identity Manager products are embedded in and execute on IBM WebSphere application server.

Product Description

Tivoli Identity Manager (TIM) interacts directly with users and with two external types of systems: identity sources and access control mechanisms. The identity systems deliver authoritative information about the users that need accounts. The provisioning system communicates directly with access control systems to create accounts, supply user information and passwords, and define the entitlements of the account. In reverse, local administrative changes made to an access control system are captured and reported to the provisioning system for evaluation against policy. Other features include:

- Role-based delegated administration allows administrative privileges to be distributed over organizational and geographical boundaries.
- Centralized Web administration
- Self-service interfaces remove the need for administrative personnel for password resets, password synchronization and the modification of personal information.
- Embedded provisioning engine and universal integration tools automate administrative

Pros

- Provides the extensive support capabilities of a large and financially secure company
- Offers many robust identity management functions.
- Utilizes a comprehensive database to store duplicate user information for each target platform
- Large installed base if previous Access360 customers are included.

Cons

- Prefers agent based approach which can lead to greater complexity and, therefore, longer implementation timeframe and increased operational cost and effort
- Agents require greater skill and effort to develop and maintain compared to agentless products.
- Large data-store of user information requires additional database infrastructure
- The recent purchases of Access360 and a meta directory solution are not yet well integrated and provide overlapping functionality

4.1.5 Lighthouse – Waveset

Company Overview

Waveset Technologies, headquartered in Austin, Texas is a leading provider of identity management software to enable the secure control of business initiatives across enterprise, intranet and extranet environments. Waveset was founded in January 2000 and acquired by SUN Microsystems in December of 2003.

Product Description

Waveset Lighthouse is a complete identity management solution that integrates provisioning management, password management, identity profile management and identity auditing. Lighthouse Enterprise Edition combines the following four solutions with an Enterprise Identity Console and Identity Platform Services:

- Provisioning Manager, a secure provisioning solution that uses automation and delegation to reduce the time and costs associated with enabling new users and instantly disables access when relationships change or end for a more secure enterprise
- Password Manager, a complete password management solution that allows end users to manage their passwords themselves, increasing their satisfaction while greatly reducing associated support costs
- Identity Broker, a identity profile management solution that easily maintains consistent identity profile information across enterprise business applications including CRM, HR and ERP applications
- Auditing and Reporting, Lighthouse's comprehensive identity auditing and reporting capabilities detect security risks and deal with them proactively.

Pros

- Agentless connections to target systems allow for simplified deployment
- Virtual Identity Manager does not require a large central repository and only 5 pieces of data per user
- A focus on standards and accreditation by utilizing standards-based interfaces based on SOAP and XML, chairing the OASIS SPML work group, being DoD COE certified, and applying for NIAP certification
- Rapidly gaining market share in the provisioning space, especially in government and financial services. Reference clients include Defense Logistics Agency, Dept. of Treasury, Merrill Lynch, and Fidelity
- Offers a government starter kit at a significant cost discount

Con

- Only possible to assign a user to one role.
- Complicated rules can be difficult to maintain.
- Specialized technical skill and training required to develop and maintain adapters.

4.2 Identity Management Product Selection Criteria

Figure 10 describes the criteria that were used to evaluate Identity Management products. The details of the evaluation for each vendor can be found in appendix E, Vendor Evaluation Criteria Matrix.

Criteria Heading	Criteria Description
Vendor Background	
Vendor Profile	Vendor profile provides a high level overview of the company and its Identity Management (IM) offering. The information collected in this category includes the size of the company, range of products, financial health and the long term viability of the vendor.
Market Profile	Vendor profile provides a high level overview of the company and its Identity Management (IM) offering. The information collected in this category includes the size of the company, range of products, financial health and the long term viability of the vendor.
Functional Requirements	
User Account Management	This criterion evaluates the user account management capabilities of the Identity Management product. The major account management functionality being evaluated is listed below: <ul style="list-style-type: none"> • Account Setup • Account Modification • Account Termination • Auditing (log changes to accounts and access privileges)
Provisioning	The provisioning capabilities of the product are evaluated in this category. The Identity Management systems ability to accept feeds from external systems is determined. IM product's ability to integrate with a security approval workflow is also evaluated.
System Administrator Management	The authentication capabilities of the Identity Management product for an administrator are evaluated in this category. IM product's access control capabilities for system administrators (in terms of auditing and delegation) are also reviewed.
Delegated Administrator Functions	An Identity Management system should provide robust delegated administration capabilities. The administrative functions should be able to be delegated by organization (e.g. by school) and functional scope (e.g. by system).
Password Policy Management	The IM product should provide the ability to create a diverse set of password rules that can be enforced. The product's password policies should be able to integrate with that of the Web Access Control product. The information collected here includes the flexibility that the product provides in enforcing different password policies within an organization.
Password Synchronization	The Identity Management product should provide the ability to synchronize passwords on different legacy and backend systems.
Self-service functions	IM product should provide users the ability to self service their accounts. The users should be able to reset their own passwords and update certain parts of their demographic information.
Registration and workflow support	Identity Management tools should be able to provide registration and workflow support for creating new user accounts. Some of the tasks that should be

Criteria Heading	Criteria Description
	<p>accomplished include:</p> <ul style="list-style-type: none"> • Accepting registration requests • Routing security requests and approvals • Workflow Capabilities
Technical Requirements	
Technical Architecture	The architecture of the product is described in this category. Information is collected on the use of agents vs. agent less approach by the product. Data regarding the complexity of the architecture, directories and databases supported is also gathered. This data helps in analyzing the compatibility of the technical architecture with internal FSA architecture.
Platform Support	The hardware platform support provided by the vendor is important to ascertain that the IM product will run on current FSA platforms.
Integration Support	Integration support information is collected to determine the products ability to support the current FSA technical environment. Information on operating systems provisioned, application provisioned and directories or databases provisioned is collected. APIs and connectors are important in a products ability to support custom and legacy applications at FSA.
Encryption	The ability of an Identity Management product to encrypt the communication to and from the managed system is vital to the security of systems at FSA. Products should be able to demonstrate the use of strong encryption methods.
Integrity Controls	<p>The integrity controls provided by an IM product are important to ensure the accuracy of data across FSA systems. Some of the major integrity control functions include:</p> <ul style="list-style-type: none"> • Error Detection • Testing Functions • Rollback Functions
Availability	Failover and high-availability function are necessary features of an IM tool. The tool should also provide load-balancing capabilities.
Central User Repository	In this category information is collected on the central store of user profile and application information. The flexibility provided in how much information should be stored by the Identity Management system can be an important consideration in selecting the appropriate tool.
Standards Support	<p>Information is collected on various standards that are supported by the product. The standard support data collected includes:</p> <ul style="list-style-type: none"> • SAML/federated identity/Liberty Alliance • Federal e-Authentication architecture • Federal authentication levels • Web Services
Product Certification	Information on federal government certification (e.g. NIAP) and industry product certifications is collected in this category.

Figure 10 – Identity Management Product Selection Criteria

4.3 Summary Evaluation Matrix – Identity Management

The table in Figure 12 is the Summary Evaluation Matrix for each vendor product in the Identity Management space. This table provides a higher level view of the vendor evaluation criteria listed in appendix E. The summary criteria evaluates the overall suitability of the product in terms of functionality, flexibility, ease of deployment, operational effort and vendor stability.

The Table below provides the key that can be used to understand the ranking given to each product in Figure 12. The details of the Summary Evaluation Matrix – Identity Management are provided in section 4.4 – Identity Management Product Analysis.






Ranking	Explanation
	Meets all defined requirements
	Meets most requirements
	Meets some requirements
	Meets only a few requirements
	Does not meet one or more critical requirements
NA	Information not available

Figure 11 – Summary Evaluation Matrix Key: Identity Management

Summary Evaluation Matrix – Identity Management

	Control SA – BMC	IdentityMinder – Netegrity	Lighthouse - Waveset	Identity Manager – Tivoli/IBM	Xellerate – Thor
Vendor Background					
Financial Profile					
Role in Marketplace					
Functional Requirements					
User Account Management					
Provisioning					
System Administrator Management					
Delegated Administrator Functions					
Password Policy Management					
Password Synchronization					
Self-service functions					
Registration and workflow support					
Technical Architecture					
General					
Platform support					
Integration support		NA			
Encryption		NA			
Integrity controls		NA			
Availability		NA			
Central User Repository		NA			
Standards support & certifications		NA			
	Control SA – BMC	IdentityMinder – Netegrity	Lighthouse – Waveset	Identity Manager – Tivoli/IBM	Xellerate – Thor
Summary Criteria					
Product Functionality		NA			
Product Flexibility		NA			
Deployment Effort		NA			
Operational Effort		NA			
Vendor Stability					
Overall Suitability for FSA					

Figure 12 – Summary Evaluation Matrix: Identity Management

4.4 Identity Management Product Analysis

All five identity management products analyzed in the previous sections represent market-leading solutions. All five products provide similar functionality, but differ in underlying architecture, platform support, and effort required for deployment and maintenance. This section details the overall summary analysis for each product as documented in the lower portion of Figure 12. This section also identifies the products recommended for additional evaluation through demonstrations in the next phase of the project.

4.4.1 Product Functionality

The five identity management products that were evaluated provide very similar functions for user administration, account provisioning, delegated administration, password policy enforcement, self-service password reset, and security approval workflow. The functions provided by these products meet or exceed the FSA business objectives and requirements identified.

4.4.2 Product Flexibility

Waveset Lighthouse seems to be the most flexible of the identity management products. Lighthouse maintains a small user repository through virtual identity management, has flexible authentication methods for administrators, does not require installation of agents on target platforms, has an auto-discovery capability to find and link identity sources, and has a fully customizable forms engine. In contrast, Tivoli Identity Manager and Control-SA generally require installation of software agents on target platforms. These products, as well as Thor Xellerate, require storage of substantially greater amounts of user data in their centralized repositories. The Thor product has an advantage in this category because of its “adapter factory” tool for quickly generating adapter interfaces for new target systems, but it suffers because it does not currently run on the HP-UX platform, a critical requirement since this platform is the new FSA standard architecture.

Netegrity recently acquired IdentityMinder (Provisioning Edition) through acquisition of Business Layers, and did not provide sufficient information for complete evaluation of product flexibility or the other factors below.

4.4.3 Deployment Effort

Waveset Lighthouse and Thor Xellerate provide the simplest deployment pathways. Xellerate offers a GUI-based Adapter Factory which simplifies the development of adapters, but it would need to be modified and certified to run under HP-UX before it would be acceptable. Lighthouse’s employs an agentless architecture and requires storing only five user data element its central repository. Tivoli Identity Manager requires additional deployment effort due to its preference for agent installation on target machines. While Control-SA offers a great deal of functionality, it has a history of long and complex deployment efforts at existing clients.

4.4.4 Operational Effort

Waveset Lighthouse and Thor Xellerate receive high marks for ease of on-going operations. Xellerate's Adapter Factory facilitates maintenance of adapters. Lighthouse's agentless architecture simplifies updates by allowing administrators to make updates only on the Identity Management systems. That way administrators are not forced to work within the testing and deployment schedules of various FSA systems. Tivoli Identity Manager requires additional operations effort due to the complexity of the product. Control-SA greater system complexity increases the maintenance effort required.

4.4.5 Vendor Stability

IBM is much larger than any of the other vendors, and offers solid financial stability for the future. BMC is next in size, and has a range of additional products outside the security category. Waveset was recently acquired by Sun. This provides additional financial stability and the opportunity to integrate the Waveset identity management product into the larger security architecture being developed by Sun. Thor is the smallest of the five companies, and is privately held. It is making significant inroads in terms of market share, but its long term future is difficult to assess. Given its current growth pattern, Thor may be a likely acquisition target.

4.4.6 Identity Management Vendor Recommendations

Based on the discussion above, the evaluation team ranks the identity management products in the following order:

1. Waveset Lighthouse
2. IBM Tivoli Identity Manager
3. BMC Control-SA
4. Netegrity IdentityMinder (Provisioning Edition)
5. Thor Xellerate

Waveset Lighthouse offers a good compromise between vendor stability, features, and deployment flexibility. Tivoli Identity Manager is a more complex product to deploy and maintain, but has the advantage of a very stable support structure available through IBM. BMC Control-SA has a full feature set, but is the most complex of the products to deploy and maintain. The Netegrity IdentityMinder (Provisioning Edition) product has a solid history as eProvision (previously marketed by Business Layers). Business Layers was recently acquired by Netegrity and the support strategy for the product is not yet clear. Thor Xellerate is an innovative product with several very attractive features, but it does not run on HP-UX.

The original Task Order for this project recommended selecting two Identity Management products to invite for more extensive demonstrations. Based on product features and vendor profiles, the Waveset and IBM Tivoli products were rated as the two highest candidates. However, because BMC Control-SA has already been licensed by

FSA (although the licenses have expired), the evaluation team recommends considering inviting the top three vendors back for the product demonstration phase.

5 Web Access Control

5.1 Introduction to Web Access Control Products

During the Tools Analysis phase, the team documented a preliminary list of Identity Management and Web Access Solutions of 10-12 vendors per product type. Initial Web Access Control solutions reviewed included:

- Assure Access (Entegriety)
- ClearTrust (RSA)
- getAccess (Entrust)
- .NET Passport (Microsoft)
- NetPoint (Obliv)
- SiteMinder (Netegrity)
- SunONE Identity Server
- Access Manager (Tivoli/IBM)
- DirectorySmart (OpenNetwork)
- Secure Access (Novell)
- SelectAccess (HP)
- WebThority (Symantec)

Each offering was initially reviewed and screened on a subset of criteria. Several products were eliminated from further consideration because of market position or technology orientation.

Entegriety is a very small vendor with limited product installations. The Entrust product had a significant market presence four years ago, but a robust development strategy was not maintained and it has declined significantly since that time. The SunONE Identity Server is a relatively new product with a small number of customers. The OpenNetworks product is optimized for Microsoft server platforms. Secure Access from Novell may be more viable in a Novell-oriented architecture, but has relatively small market presence. SelectAccess was recently acquired by HP from Baltimore Technologies, which is liquidating its assets, and it is too soon to tell how vigorously it will be supported. WebThority by Symantec has few customers, does not feature market-leading functionality, and is not being vigorously marketed.

Given the above considerations, four web access control vendors were selected for further consideration, and are described in greater detail in following sections. These products were also assessed to be the market leaders in analyses conducted by both Gartner and the Meta Group. They are:

- ClearTrust (RSA)
- NetPoint (Obliv)
- SiteMinder (Netegrity)
- Access Manager (Tivoli/IBM)

5.1.1 SiteMinder – Netegrity

Company Overview

Netegrity, Inc., founded in 1986, is a publicly held company headquartered in Waltham, Mass. Netegrity solutions are licensed to more than 250 million users at over 700 organizations worldwide, including more than half of the Fortune 100. Customers include Aetna, American Express, Bank One, E*TRADE, General Electric, the Internal Revenue Service, USDA, and Wells Fargo. Netegrity is a mature company in the web access control market space with a large corporate and government customer base.

Product Description

Netegrity SiteMinder is a software platform of shared services that enables single sign-on and policy based centralized control of user authentication and access management. Key components of SiteMinder are listed below:

- SiteMinder Policy Server determines which form of authentication is required. SiteMinder supports a wide range of authentication methods including passwords, smart cards, certificates, and tokens, as well as combinations of these methods.
- SiteMinder Web Agents (Web Server Filters) reside on the Web server or other resource that is being protected and intercept incoming requests for content. The filters check if the requestor has been authenticated and authorized. If the requestor has not yet been authenticated, the Web agent will manage the requests and responses between the user and the Policy Server.
- SiteMinder's Secure Proxy Server is similar to a SiteMinder agent and follows the same basic steps when working with the SiteMinder Policy Server to provide authentication and authorization.

Pros

- Extensive Web Access Control functionality and history of rapid deployments
- A consistent #1 or #2 product ranking by leading industry analysts
- SiteMinder's large install base including major government agencies and financial institutions
- A robust set of developer tools increase SiteMinder's flexibility to meet unique requirements
- Flexible rules and roles based administration
- Supports security industry standards (e.g. SAML)
- Strong customer service capabilities

Con

- Does not provide advanced testing and roll-back functions
- Login page requires SiteMinder proprietary code embedded with the HTML for processing by the Policy Server
- Company revenue is only from security product offerings

5.1.2 NetPoint – Oblix

Company Overview

Oblix, Inc., founded in 1996, is a privately held company headquartered in Cupertino, California. Oblix is currently being lead by former executives from BEA WebLogic, Sun Microsystems, Oracle, Silicon Graphics, Symantec, Inktomi, and Ask Jeeves. Relevant customers include United States Postal Service (USPS), Dept. of Navy, Dept of Energy, Washington Mutual, Goldman Sachs, and the US Army.

Product Description

NetPoint Access System enforces access policies for Web applications and content through policy-based authentication, authorization, and auditing. Key components:

- NetPoint Access Server which provides authentication, authorization, and auditing services and supports various authentication methods.
- NetPoint Access Manager lets administrators manage and delegate policy administration.
- NetPoint WebGate (Web Server Filters) acts as the interface between individual Web servers and the NetPoint Access Server.
- NetPoint COREid System provides a customizable identity workflow engine and identity and policy delegation for individual users or groups of users.
- NetPoint SHAREid facilitates identity federation and security. The FederatedID Layer provides a SAML system that is integrated with the COREid identity management functionality enabling the extension of single sign-on to affiliate partners.

Pros

- NetPoint provides a flexible product architecture which lessens the difficulty of deployment and on-going operations
- Oblix is actively involved in the Federal eAuthentication project
- Oblix has been in the identity management space since its inception in 1996.
- Oblix NetPoint is the only identity and Web access management solution built on XML-Based Web services architecture.
- NetPoint offers native integration with Active Directory and integrated Windows authentication (Oblix is a Microsoft Certified Partner).

Cons

- Does not support HP-UX platform.
- Least integrated from a third party provisioning tool perspective.
- Oblix is a smaller company as compared to the other vendors.
- Single revenue stream from security product offerings.

5.1.3 ClearTrust – RSA

Company Overview

RSA, founded in 1984, is a publicly held company based in Bedford, MA. In 2001, RSA acquired Securant and became a player in the Single Sign-On space. Customer base includes Lehman Brothers, Wells Fargo, ARMY/PEO, NSA, GSA eAuthentication project, Navy Medical Logistics and Nationwide Insurance. RSA has a large security customer base, primarily for its other security products (SecurID and PKI tools), with 9,000 customers and a wide range of experience in government.

Product Description

RSA ClearTrust Web access management solution helps enable secure access to Web-based resources providing users with single sign-on across multiple applications. Key components of the ClearTrust Product include:

- Authorization Server performs the authentication and Web access management checks for users at runtime.
- Entitlements Server is the central server for the administrative functionality of the RSA ClearTrust system.
- Data Abstraction Layer allows data to be leveraged in its native format, whether that is an LDAP directory or a SQL database.
- Web Server Agents (Web Server Filters) forward access requests to an RSA ClearTrust Authorization Server which then passes the allow/deny response it receives back to the Web server.
- Entitlements Manager is the administrative tool used to manage the data that controls the entire RSA ClearTrust system. The Entitlements Manager sets up groups and roles, add resources, or define security policies

Pros

- Strong security between Access Control components
- Integrates with all major Identity Management solutions - integrates with Thor's Xellerate product as an Accelerated Delivery Methodology
- Mature, trusted, and innovative company in the broader security market space
- Supports SAML and other federated identity standards

Cons

- The ClearTrust product does not provide as much flexibility as the other products
- The deployment of the ClearTrust product can be complex
- Smaller number of active implementations compared to other vendors.

5.1.4 Access Manager – Tivoli/IBM

Company Overview

IBM's software offerings, branded as Tivoli, provide an end to end package of tools for integrating, managing, and securing an enterprise's security infrastructures. Customer base for IBM's Access Manager includes Shell Canada, T. Rowe Price, AT&T, and the US Air Force. IBM's strength and dominance in the application server market gives Tivoli an advantage in the enterprise space. Both the Access Manager and Identity Manager products are embedded in and execute on IBM WebSphere application server.

Product Features

IBM Tivoli Access Manager provides Web single sign-on, distributed Web-based administration, and policy-based security. Key components of Access Manager include:

- Access Manager Policy Server maintains the master authorization database for the secure domain. This server is vital to the processing of access control, authentication, and authorization requests.
- Authorization Database (Proprietary database bundled with the Policy Server) is used for authorization functions. It is separate from the User Registry and contains a virtual representation of the resources it protects.
- WebSeal Server is a reverse proxy that applies a security policy to a protected resource. WebSeal can provide single sign-on solutions and incorporate back-end Web application server resources into its security policy.

Pros

- Provides the extensive support capabilities of a large and financially secure company
- Has a large install base. Most customers implement by utilizing the web seal reverse proxy server
- Is consistently ranked as the #1 or #2 product by leading industry analysts
- Access Manager and Identity Manager support is well integrated since both products are owned by IBM

Cons

- Offers many customizable implementation options.
- Product complexity and use of a proprietary schema may make implementation more difficult
- Prefers the use of WebSeal reverse proxy server, requiring additional hardware and network components for implementation
- Security products represent small percentage of supported software products
- Extensive hardware needed to support the architecture (requires the most components as compared to the other vendors)
- Additional IBM specific components are required (i.e. MQ Series)

5.2 Web Access Control Product Selection Criteria

The table in Figure 13 below describes the criteria that were used to evaluate Web Access Control products. The details of the evaluation for each vendor can be found in appendix E, Vendor Evaluation Criteria Matrix.

Criteria Heading	Criteria Description
Vendor Background	
Vendor Profile	Vendor profile provides a high level overview of the company and its Web Access Control (WAC) offering. The information collected in this category includes the size of the company, range of products, financial health and the long term viability of the vendor. These factors help in judging the long term prospects of the vendor and its ability to provide continuing support for the product at FSA.
Market Profile	This category collects information about the product's market penetration and the relevant reference install base for this vendor. Market penetration data allows the team to judge the current acceptance of the product in the industry. High penetration rate might suggest the product provides features and benefits that are embraced by customers.
Functional Requirements	
User Authentication	That data collected in the user authentication category includes the types of authentication mechanisms that are supported by the product. Information on the product's ability to support remote calls and to provide customizable user log-in interfaces is also included.
Single Sign-On	Single Sign-On criteria evaluates a product's ability to provide effective session management and Cross-site sign-on capabilities. Within this criterion, the Web Access Control (WAC) product is also judged on its ability to provide transitive trust functionality.
User Access Control	User Access Control criteria collects information about the different attributes based on which access is granted by the product. The example of these attributes includes Access Controls Lists (ACLs), role based access and rule based access (e.g. real time decision making). Flexible mechanisms for user access control can allow for ease of integration with current roles and groups within the organization.
User Auditing and Reporting	Auditing and reporting functions provide the ability to capture and record user actions. These reports can be used to ensure compliance with FSA's policies. The information collected in this category includes: <ul style="list-style-type: none"> • Actions that can be audited by the product • Administrator interface used for configuring auditing capabilities • Security controls for audit logs • Interface for configuring report capabilities
Administrative Management	The data collected in this category includes administrative authentication, administrative access control and administrative auditing and reporting capabilities. The information provided above can be used to judge the robustness of the product in regards to administrative controls.
Administrative Interface	The following information is collected about the administrative interface of the WAC product: <ul style="list-style-type: none"> • Type of client used

Criteria Heading	Criteria Description
	<ul style="list-style-type: none"> Complexity / Usability/Training requirements Customizability of the interface
Enforce Password Policies	The information collected here includes the flexibility that the product provides in enforcing different password policies within an organization. The ability of a product to cross check user passwords against a customized dictionary can be beneficial to FSA.
Technical Requirements	
Technical Architecture	The architecture of the product is described in this category. Information is collected on the use web agents and plug-ins by the product. Data regarding use of reverse proxy, use of cookies and credential caching is also collected.
Platform Support	The hardware platform support provided by the vendor is important to ascertain that the WAC product will run on current FSA platforms.
Integration Support	Integration support information is gathered to determine the products ability to support the current FSA technical environment. Information on Web Server and application server support is collected for each vendor. Data regarding user directory and database support for security repositories is also provided. APIs and connectors are important in a products ability to support custom and legacy applications at FSA.
Security Features	The security features of the WAC tool itself are an important factor in selecting the right product. The inter-component communication should be encrypted using an industry/government accepted algorithm. These products should also provide intrusion detection functionality.
Integrity Controls	The WAC tool should provide integrity control functions to detect errors, test functions and rollback functions.
Availability	Failover and high-availability function are necessary features of a WAC tool. The tool should also provide load-balancing capabilities.
Central User Repository	In this category information on types of security data stores used by the WAC products is collected. A list of database and directories that are supported by the vendor is provided. Other information on central user store is also collected including additional user attributes that can be configured.
Standards Support	<p>Information is collected on various standards that are supported by the product. The standard support data collected includes:</p> <ul style="list-style-type: none"> SAML/federated identity/Liberty Alliance Federal e-Authentication architecture Federal authentication levels Web Services
Product Certification	Information on federal government certification (e.g. NIAP) and industry product certifications is collected in this category.

Figure 13 – Web Access Control Product Selection Criteria

5.3 Summary Evaluation Matrix – Web Access Control

The table in Figure 15 is the Summary Evaluation Matrix for each vendor product in the Web Access Control space. This table provides a higher level view of the vendor evaluation criteria listed in Appendix E. The summary criteria evaluates the overall suitability of the product in terms of functionality, flexibility, ease of deployment, operational effort and vendor stability.

The Table below provides the key that can be used to understand the ranking given to each product in Figure 15. The details of the Summary Evaluation Matrix – Web Access Control are provided in section 5.4 – Web Access Control Product Analysis.






Ranking	Explanation
	Meets all defined requirements
	Meets most requirements
	Meets some requirements
	Meets only a few requirements
	Does not meet one or more critical requirements

Figure 14 – Summary Evaluation Matrix Key: Web Access Control

Summary Evaluation Matrix – Web Access Control

	Clear Trust – RSA	NetPoint – Oblix	SiteMinder – Netegrity	Access Manager – Tivoli/IBM
Vendor Background				
Financial Profile				
Role in Marketplace				
Functional Requirements				
User Authentication				
Single Sign-On				
User Access Control				
User Auditing and Reporting				
Administrator Management				
Administrator Interface				
Enforces Security Policies				
Technical Architecture				
General				
Platform support				
Integration support				
Security features				
Integrity controls				
High Availability				
Central User Repository				
Standards support & certifications				
	Clear Trust - RSA	NetPoint – Oblix	SiteMinder – Netegrity	Access Manager – Tivoli/IBM
Summary Criteria				
Product Functionality				
Product Flexibility				
Ease of Deployment				
Operational Effort				
Vendor Stability				
Overall Suitability for FSA				

Figure 15 – Summary Evaluation Matrix: Web Access Control

5.4 Web Access Control Product Analysis

The four web access control products chosen for initial evaluation are market leaders, according to both independent analysts and by virtue of their market penetration. While similar in overall functionality, there are significant differences between these products in their design approach. This section discusses the rationale behind the overall rankings shown in Figure 15. This section also explains the team recommendations for products to invite back for the demonstration phase of this project.

5.4.1 Product Functionality

All four web access control products include web application security functions for user authentication, single sign-on, session management, authorization, and auditing. The web security functions provided by these products meet or exceed those required to satisfy FSA business objectives.

5.4.2 Product Flexibility

Netegrity Siteminder offers the most flexibility while integrating with all major directory services and possessing good application rules, role administration, and fine-grain access. IBM's Tivoli Access Manager is highly customizable and offers a very large number of options for authentication and authorization. RSA ClearTrust and Oblix NetPoint offer good flexibility with support of various authentication methods and customizable web-based interfaces, but the Oblix product does not support the HP-UX platform.

5.4.3 Deployment Effort

Netegrity has a history of rapid deployments, due in part to its web agent architecture, and offers a robust set of developer tools to meet custom requirements. IBM's Tivoli Access Manager provides support for both proxy and agent based architectures but is historically implemented with a reverse web proxy (WebSeal). As a result, Tivoli Access Manager has a history of more difficult implementations due to its increased complexity. RSA has a web agent architecture, but has a record of more difficult implementations. Oblix's web agent based architecture has also led to recent quick deployments, but the need to modify and certify this product to run on HP-UX would significantly complicate implementation.

5.4.4 Operational Effort

Netegrity's web server agents are simpler to maintain than a reverse proxy architecture. Oblix NetPoint and RSA ClearTrust also choose server agents over a reverse proxy approach. Tivoli Access Manager's highly customizable implementation options and proprietary directory schema can be more difficult to maintain.

5.4.5 Vendor Stability

Of the four vendors, IBM is the most stable company financially. Netegrity is smaller than IBM, but has a solid history of steady growth. Netegrity concentrates on security products, and recently purchased the identity management vendor Business Layers. RSA

has a diversified security product offering that includes authentication tokens and PKI products. RSA appears to be maintaining its installed base, but has a much lower market penetration than Netegrity or IBM. While the other three vendors are public companies, Oblix is a private company funded by venture capital. As its market presence grows, it will become a likely acquisition target.

5.4.6 Web Access Control Vendor Recommendations

Based on the previous vendor characteristics, the evaluation team ranks the web access control products in the following order:

1. Netegrity Siteminder
2. IBM Tivoli Access Manager
3. RSA ClearTrust
4. Oblix NetPoint

Netegrity SiteMinder offers a stable product with a comprehensive set of authentication, authorization, and single sign-on features. It is based on a web agent architecture, which promotes a simpler and more rapid deployment. Unlike the other three products, the IBM web access control product prefers implementation with the reverse proxy architecture. This would require deployment of additional network hardware in the FSA environment, and requires more effort for scaling to support increased traffic loads. The RSA ClearTrust product is solid, but it currently has fewer customers than Netegrity or the Tivoli product. Oblix NetPoint is a newer product, but it provides a full feature set and has developed a reputation for rapid deployments. However, its lack of support for running on HP-UX makes it currently unsuitable for selection by FSA.

The evaluation team recommends inviting Netegrity and IBM Tivoli for the next demonstration phase. RSA could optionally be added to this list to provide an additional alternative if FSA decides that the reverse-proxy architecture is not acceptable for the FSA environment.

6 Conclusion and Next Steps

Based on the product evaluation criteria, several solutions in each category are recommended for further product demonstrations and evaluations during the Products Option Phase.

Identity Management:

1. *Waveset Lighthouse* offers a good compromise between features, deployment flexibility, and vendor stability.
2. *IBM's Tivoli Identity Manager* is a more complex product to deploy and maintain, but has the advantage of a very stable support structure.
3. *BMC's Control-SA* did not rank as high as the previous two products because of its more complex deployment and maintenance requirements.

The original Task Order for this project recommended selecting two Identity Management products to invite for more extensive demonstrations. However, because Control-SA was licensed in the past by FSA, it was also added to the list of vendors to invite for on-site demonstrations.

Web Access Control:

1. *Netegrity SiteMinder* offers a stable product with a comprehensive set of authentication, authorization, and single sign-on features.
2. *IBM Tivoli Access Manager* is based on a reverse-proxy architecture, and has a comprehensive feature set, although its complexity has led to complicated deployment efforts for some customers.
3. *RSA ClearTrust* has a smaller installed base than either of the two previous products, but is stable and supported by a vendor with a very strong presence in the security product market.

The RSA product was added to this list to provide an additional alternative product in the event that the reverse-proxy architecture is found unsuitable for the FSA environment.

Industry analyst research supports the recommendation of these Identity Management and Web Access Control tools for further evaluation by FSA. These tools are rated among the top of their peer group and possess the functionality necessary to meet or exceed FSA Business Objectives.

The Product Options Phase will include:

- A detailed product demonstration by each vendor.
- Observation and evaluation of product installation.
- The collection of additional data on product functionality and evaluation of features.

At the conclusion of the Product Options Phase, a single Identity Management tool and a single Web Access Control tool will be selected for the Prototype Phase. The Product

Options Phases will be complete by March 5, 2004. In the Prototype Phase, the Identity Management and Web Access Control solution will be prototyped in the FSA development environment and tested against FSA business objectives using a test copy of ezAudit. The Prototype Phase will be complete by May 14, 2004.

Appendix A: Enrollment and Access Management Solution Vision

Figure 16 depicts the Enrollment and Access Management solution vision for FSA. This solution resulted from the 123.1.27 - Access Management Business Objectives (11/30/03) deliverable.

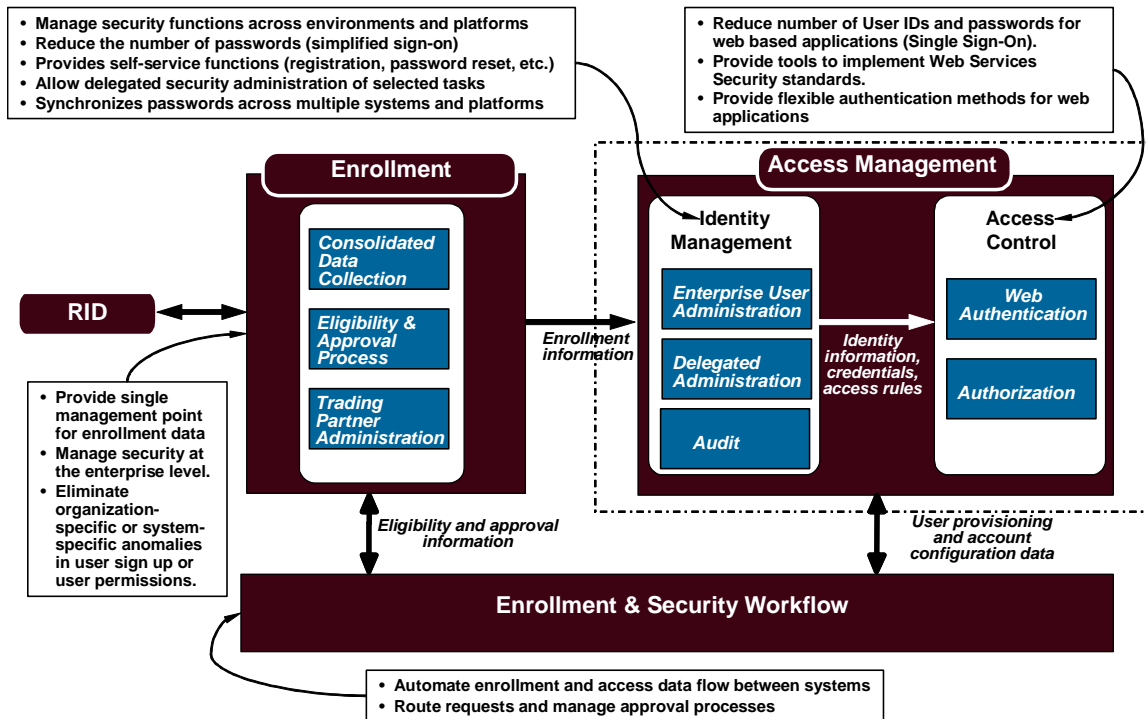


Figure 16 – FSA Identity and Access Management Solution Vision

Appendix B: FSA Security and Privacy Architecture Framework

FSA Security and Privacy Technical Architecture Vision resulted from 124.1.3 - Security and Privacy Architecture Framework Specification (5/30/03) deliverable. Appendix B below depicts this vision.

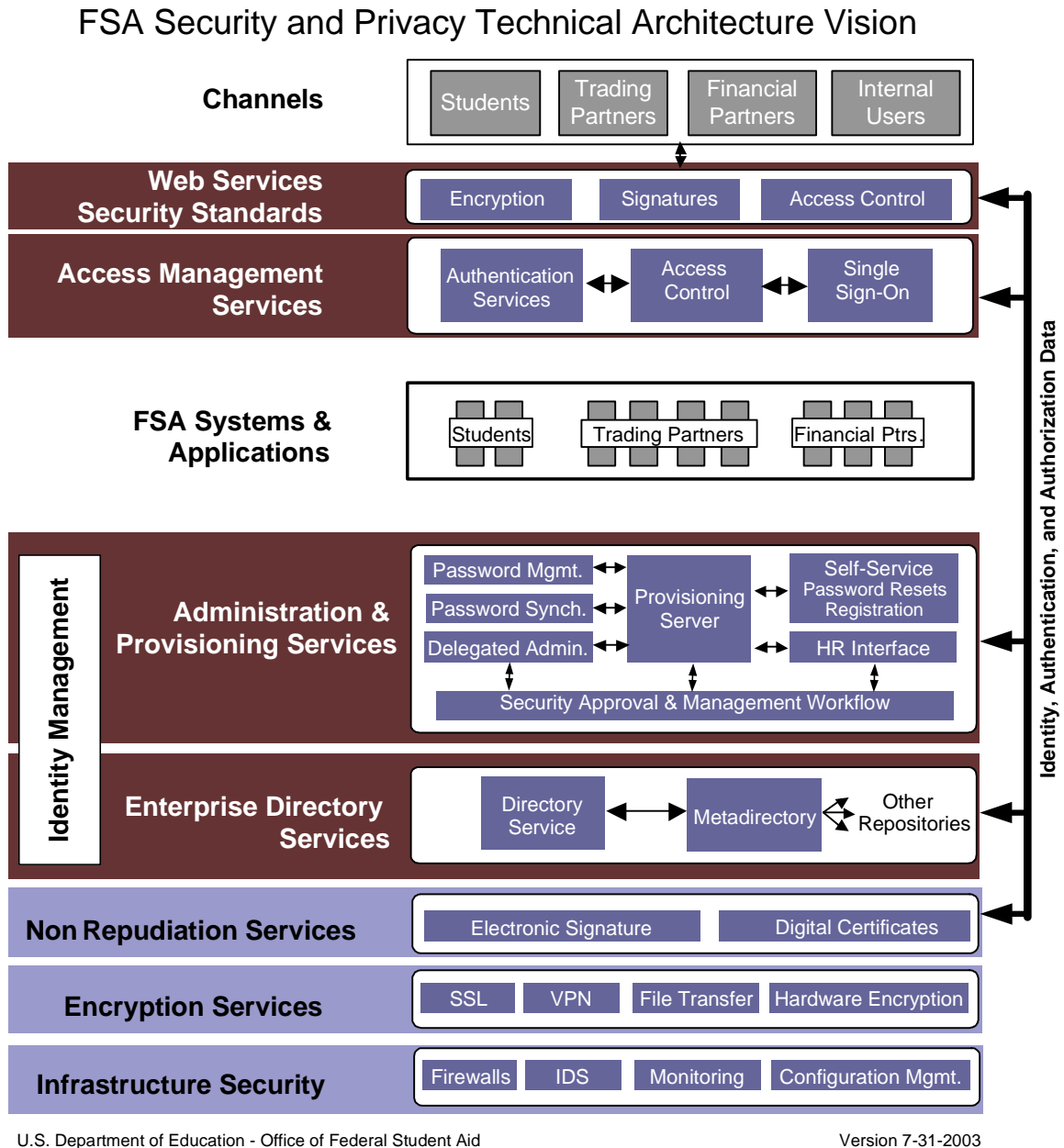


Figure 17 – FSA Security and Privacy Technical Architecture

Appendix C: Security Working Group Roster

Figure 18 provides the list of members who are in the Security Working Group for Identity and Access Management Tools analysis at FSA.

Core Team Members	
Name	Organization
Rosemary Beavers	COD
Mike Fillinich	CIO
Paul Hill	Data Strategy
Jay Hurt	CFO
Bob Ingwalson	CIO
Ganesh Reddy	CIO
Jeanne Saunders	CPS
Keith Wilson	CIO
Molly Wyatt	PEPS/IPM

Other Participants	
Name	Organization
David Elliott	CIO
Matteo Fontana	FP
Chris Hill	PEPS
Denise Hill	CIO
John Hsu	VDC
Pamela Jefferson	FMS
William Leith	FMS
Jay Long	PEPS
Schonda Piper	DLSS/CSB
Shirley Pratt	FMS
Brian Sullivan	DCSS
Dwight Vigna	DLSS
Steve Wingard	COD
Randy Wolff	ezAudit
Terry Woods	CIO

Figure 18 - Security Architecture Workgroup Roster

Appendix D: Security Working Group Presentation

Appendix D list the Identity and Access Management Tools Analysis project status report presentation made to the Security Working Group on Jan. 14.

Refer to the “Appendix D Security Working Group Presentation.ppt” file

Appendix E: Vendor Evaluation Criteria Matrix

Appendix E list the detail evaluation criteria and results for each of 9 products reviewed in Identity and Access Management Tools – Vendor Analysis deliverable.

Refer to the “Appendix E Vendor Evaluation Criteria Matrix v1.0.xls” file